Strategic Investments Research Program

Technical Accomplishment

High-Assurance Software Design

POC: Michael Lowry (Ames Research Center)
February 2002

Relevant Milestone: Demonstrate scalable analytic verification technology on a major subsystem for Aerospace avionics.

Shown: The application of model checking to the DEOS real-time embedded aerospace operating system from Honeywell to discover a subtle error not uncovered using the testing techniques required for FAA certification. This impact of this error during flight could have been starvation of critical real-time flight calculations. Indicate the scaling of model checking by showing the average factor of increase in lines of code (yellow) and state-space handled (white) by each technique developed and, in the middle, a graph indicating the impact of these techniques with respect to the time taken to analyze a 1000 lines of code.

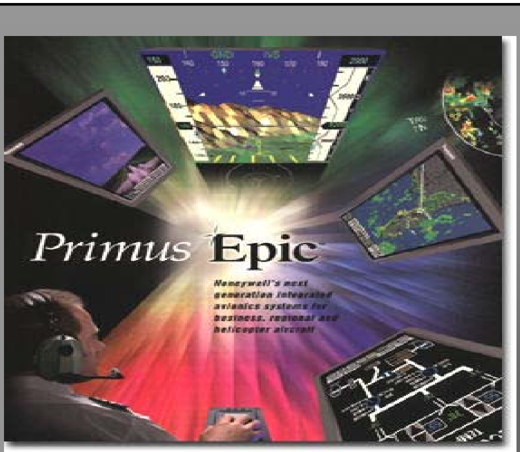
Accomplishment / Relation to Milestone and ETG: Development of the Java PathFinder model checker, with accompanying set of synergistic verification technologies (including, abstractions, slicing, partial-order reduction, intelligent search and environment generation techniques) to enable the efficient analysis of object-oriented, concurrent programs such as those found in the next generation of avionics systems (e.g. the DEOS O/S for Integrated Modular Avionic systems). These model checking technologies have significantly reduced the effort required to analyze avionics software: currently we analyze 1000 lines of code per day compared to state of practice of 50 LOC/day in 1998.

Future Plans: Develop techniques to allow guarantees for correct behavior under certain assumptions that can be checked during actual execution using run-time program monitoring. Also, development of "learning" algorithms whereby the model checker's search strategy can be adapted according to the structure of the program being analyzed.

ETG: Provide increased confidence and lower the cost of development of next generation avionics software

Strategic Investments Research Program

High-Assurance Software Design


Primus Epic
Honeywell's next generation integrated avionics systems for business, regional and helicopter aircraft

DEOS
10000 lines to 1500

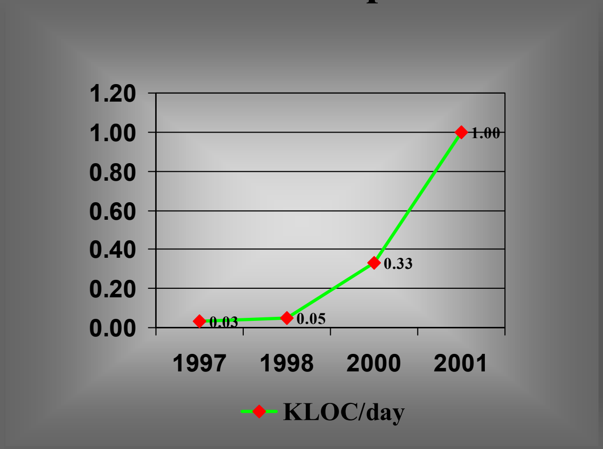
3x **Slicing** 30x

Property preserving

Case 0:
new();
Case 1:
Stop();
Case 2:
Remove();
Case 3:
Wait();

Repair

Combined techniques allows $O(10^2)$ source line and $O(10^6)$ state-space increase over state of practice



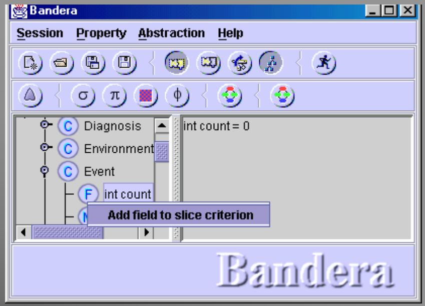
5x **Abstraction** 100x

DEOS
Infinite state to 1,000,000 states

Environment Generation

Semi-automated and requires domain knowledge

Bandera code-level debugging of error-path



Spurious error elimination during abstraction

2x 10x
Heuristic search
Focused search for errors

JPF Model Checker

State compression
2x 15x

Partial-order reduction
2x 10x

Case 0:
new();
Case 2:
Remove();